UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

AMOR CARO DEL CASTILLO, *individually and on behalf of all others similarly situated*, Plaintiff, v. IHEARTMEDIA + ENTERTAINMENT, INC. and IHEARTMEDIA, INC., Defendants.	5:25-cv-00538 **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Amor Caro Del Castillo ("Plaintiff"), on behalf of herself and all others similarly situated ("Class Members"), alleges the following against Defendants iHeartMedia + Entertainment, Inc. ("IHME") and iHeartMedia, Inc. ("IHM") (collectively, "Defendants"), upon Plaintiff's personal knowledge and upon information and belief, including the investigation of counsel.

I. INTRODUCTION

1. This action arises from Defendants' failure to safeguard the sensitive Personally Identifiable Information[1] ("PII") and Protected Health Information ("PHI") (collectively, "Private Information") of Plaintiff and the proposed Class Members that was impacted in a data breach that Defendant IHME publicly disclosed on April 30, 2025 (the "Data Breach" or the "Breach).

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

2. Plaintiff's claims arise from Defendants' failure to properly secure and safeguard Private Information that was entrusted to them, and their accompanying responsibility to store and transfer that information.

3. Defendant IHME is a multimedia company that owns and operates radio stations and manages outdoor and indoor events.

4. Defendant IHM is an American mass media corporation.

5. Defendants had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on their affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

6. Between December 24, 2024, and December 27, 2024, an unauthorized third-party viewed and obtained filed stored on systems of a number of Defendant IHME's local stations.[2] In response, Defendant IHME launched an investigation to determine the nature and scope of the Data Breach.[3]

7. On April 11, 2025, Defendant IHME's investigation determined that certain files containing sensitive Private Information were exposed in the Data Breach.[4]

8. Upon information and belief, the following types of Private Information were compromised as a result of the Data Breach: name, Social Security number, tax identification number, driver's license number, and/or state identification card number.[5] Additionally, the following Private Information may have been compromised: passport number or other

[2] Exhibit 1: Amor Caro Del Castillo's Notice Letter.
[3] *Id.*
[4] *Id.*
[5] *Id.*

governmental identification number, data of birth, financial account information, payment card information, health information and/or health insurance information.[6]

9. On April 30, 2025, Defendant IHME issued a notice of public disclosure and began sending notice letter to individuals impacted by the Data Breach.[7]

10. Defendants failed to take precautions designed to keep individuals' Private Information secure.

11. Defendants owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendants solicited, collected, used, and derived a benefit from the Private Information, yet breached their duty by failing to implement or maintain adequate security practices.

12. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

13. Defendants, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' Private Information.

14. As a result of Defendants' inadequate digital security and notice process, Plaintiff's and Class Members' Private Information was exposed to criminals. Plaintiff and the Class Members have suffered and will continue to suffer injuries, including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private Information as a

---

[6] *Id.*

[7] *Data Breach Notifications*, iHeartMedia + Entertainment, Inc., OFFICE OF THE MAINE ATTORNEY GENERAL: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/79b5d25d-ddf1-4f01-802d-1b8c43010377.html (last visited May 5, 2025).

result of the Data Breach; uncompensated necessary lost time associated with detecting and preventing identity theft; and, theft of personal and financial information.

15. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendants' failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendants' conduct amounts to at least negligence and violates federal and state statutes.

16. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendants for: negligence; breach of implied contract; unjust enrichment; breach of fiduciary duty; and invasion of privacy.

17. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

II. PARTIES

15. Plaintiff Amor Caro Del Castillo is a citizen and resident of Spring Valley, California.

16. Defendant iHeartMedia + Entertainment, Inc. is a Nevada corporation maintaining its principal place of business located at 20880 Stone Oak Parkway, San Antonio, Texas 78258. The registered agent for service of process is CT Corporation System, 1999 Bryan St., Suite 900, Dallas, Texas 75201.

17. Defendant iHeartMedia, Inc. is a Delaware corporation maintaining its principal place of business at 20880 Stone Oak Parkway, San Antonio, Texas 78258. The registered agent for service of process is CT Corporation System, 1999 Bryan St., Suite 900, Dallas, Texas 75201.

III. JURISDICTION AND VENUE

18. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is more than 100 and at least one member of the Class defined below is a citizen of a different state that is diverse from Defendants' citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332 (d) (2) (A).

19. This Court has personal jurisdiction over Defendants because Defendants are registered to do business and maintain their principal places of business in this District.

20. Venue is proper in this Court because Defendants maintain their principal places of business in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Background on Defendants

21. Defendant IHME is a multimedia company that owns and operates radio stations and manages outdoor and indoor events.

22. Defendant IHM is an American mass media corporation.

23. Upon information and belief, Defendants made promises and representations to individuals, including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

24. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectations and on the mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

25. As a result of collecting and storing the Private Information of Plaintiff and Class Members for their own financial benefit, Defendants had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' Private Information from disclosure to third parties.

B. The Data Breach

26. Between December 24, 2024, and December 27, 2024, an unauthorized third-party viewed and obtained filed stored on systems of a number of Defendant IHME's local stations.[8] In response, Defendant IHME launched an investigation to determine the nature and scope of the Data Breach.[9]

27. On April 11, 2025, Defendant IHME's investigation determined that certain files containing sensitive Private Information were exposed in the Data Breach.[10]

28. Upon information and belief, the following types of Private Information were compromised as a result of the Data Breach: name, Social Security number, tax identification number, driver's license number, and/or state identification card number.[11] Additionally, the following Private Information may have been compromised: passport number or other governmental identification number, data of birth, financial account information, payment card information, health information and/or health insurance information.[12]

[8] Exhibit 1: Amor Caro Del Castillo's Notice Letter.
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*

29. On April 30, 2025, Defendant IHME issued a notice of public disclosure and began sending notice letter to individuals impacted by the Data Breach.[13]

30. Defendants failed to take precautions designed to keep individuals' Private Information secure.

31. While Defendants sought to minimize the damage caused by the Data Breach, they cannot and have not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

32. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendants' Failure to Prevent, Identify, and Timely Report the Data Breach

33. Defendants failed to take adequate measures to ensure individuals' Private Information was protected against unauthorized access.

34. The Private Information that Defendants allowed to be exposed in the Data Breach are the types of private information that Defendants knew, or should have known, would be the target of cyberattacks.

35. Despite their own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[14] Defendants failed to disclose that their systems and security practices were inadequate to reasonably safeguard individuals Private Information.

---

[13] *Data Breach Notifications*, iHeartMedia + Entertainment, Inc., OFFICE OF THE MAINE ATTORNEY GENERAL: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/79b5d25d-ddf1-4f01-802d-1b8c43010377.html (last visited May 5, 2025).

[14] *Protecting Personal Information: A Guide for Business,* FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited May 5, 2025).

36. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[15] Immediate notification of a data breach is critical so that those impacted can take measures to protect themselves.

37. Here, Defendant IHME waited nearly three weeks after being made aware of the Data Breach to notify impacted individuals.

D. The Harm Caused by the Data Breach Now and Going Forward

38. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[16]

39. The types of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft.

40. Plaintiff and Class Members face a substantial risk of identity theft given that their Private Information was compromised in the Data Breach.

41. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

---

[15] *Id.*

[16] *Prevention and Preparedness*, New York State Police, https://troopers.ny.gov/prevention-and-preparedness (last visited May 5, 2025).

42. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.[17]

43. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity."[18] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[19]

44. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21]

45. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[22]

---

[17] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited May 5, 2025).

[18] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited May 5, 2025).

[19] *Id.*

[20] *Id.*

[21] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited May 5, 2025).

[22] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-

46. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[23] Defendants did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen. Defendant IHME notified impacted individuals nearly three weeks after learning of the Data Breach.

47. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendants' Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendants with the mutual understanding that Defendants would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendants, and which is subject to further injurious breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited May 5, 2025).

[23] *Id.*

48. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

49. Defendants disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

50. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendants' wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

E. Plaintiff Amor Caro Del Castillo's Experience

51. Plaintiff is a customer of Defendants. On April 30, 2025, Defendants sent Plaintiff a notice letter informing her that her Private Information was compromised in the Data Breach.

52. Defendants were in possession of Plaintiff's Private Information before, during and after the Data Breach.

53. Plaintiff reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff would not have allowed Defendants, or anyone in Defendants position, to maintain her Private Information if he believed that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

54. Plaintiff greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

55. Plaintiff stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

56. To the best of Plaintiff's knowledge, her PII has not been compromised in a prior data breach.

57. As a result of the Data Breach, Plaintiff has spent considerable and necessary time researching the Data Breach, reviewing her bank accounts, monitoring her credit report, changing

her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

58. As a consequence of and following the Data Breach, Plaintiff has experienced a significant uptick in spam calls, text messages, and emails.

59. The Data Breach has caused Plaintiff to suffer anxiety and stress.

60. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present and continued increased risk of identity theft and fraud for years to come.

61. Plaintiff has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendants possession, are protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

62. Plaintiff brings this nationwide class action individually and on behalf of all other persons similarly situated ("Class") pursuant to Federal Rule of Civil Procedure 23(a) and 23(b)(3).

63. Plaintiff proposes the following nationwide Class definition, subject to amendment based on information obtained through discovery:

> All individuals whose Private Information was impacted in Defendants Data Breach that occurred in April 2025.

64. Excluded from the Class are Defendants officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

65. Plaintiff reserves the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

66. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Class Members' claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

67. This action satisfies the requirements for a class action under Federal Rule of Civil Procedure 23(a)(1)–(3) and 23(b)(2), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

68. **Numerosity, Rule 23(a)(1):** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, thousands of individuals were impacted by the Data Breach. Such information is readily ascertainable from Defendants records.

69. **Commonality, Rule 23(a)(2):** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act and HIPAA;

d. Whether Defendants data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether hackers obtained Plaintiff's and Class Members' Private Information in the Data Breach;

f. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

g. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants misconduct;

h. Whether Plaintiff and the Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

70. **Typicality, Rule 23(a)(3):** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

71. **Adequacy, Rule 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel is competent and experienced in litigating data breach class actions.

72. **Predominance, Rule 23(b)(3):** Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and all Class Members' Private

Information was stored on the same computer systems and unlawfully exposed in the same way. The common issues arising from Defendants conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

73. **Superiority, Rule 23(b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions.

b. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

c. When the liability of Defendants have been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendants to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

d. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by

Defendants, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendants.

74. In addition, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

75. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely and adequately notify the public of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendants security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard individuals Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

76. Finally, all members of the proposed Class are readily ascertainable, as Defendants have access to Class Members' names and addresses affected by the Data Breach.

CAUSES OF ACTION

COUNT I: NEGLIGENCE
(On Behalf of Plaintiff and the Class)

77. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 17, and 21 through 61, as if fully set forth herein.

78. Defendants required Plaintiff and Class Members to submit private, confidential Private Information to Defendants as a condition of receiving services from Defendants.

79. Defendants had full knowledge of the sensitivity of the Private Information to which it was entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons. Defendants had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that Private Information.

80. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices by Defendants.

81. Plaintiff and the Class Members had no ability to protect their Private Information in Defendants possession.

82. By collecting and storing Plaintiff's and Class Members' Private Information in their network server(s), Defendants had a duty of care to use reasonable means to secure and safeguard it, to prevent its unauthorized disclosure, and to safeguard it from theft. Defendants duty included a responsibility to implement processes by which they could detect if that Private Information was exposed to the internet and to give prompt notice to those affected in the case of a data breach.

83. Defendants owed a duty of care to Plaintiff and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

84. Defendants duty of care to use reasonable security measures arose because of the special relationship that existed between Defendants and consumers, which is recognized by statutes and regulations including but not limited to the FTC Act, HIPAA, as well as common law. Defendants were able to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach, yet failed to do so.

85. Defendants had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

86. Pursuant to the FTC Act, 15 U.S.C. § 45 *et seq.*, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

87. Further, pursuant to HIPAA, 42 U.S.C. § 1302d *et seq*., Defendants had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

88. In additional, under HIPAA Defendants had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* 45 C.F.R. § 164.304.

89. Defendants breached their duties to Plaintiff and Class Members and violated the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

90. The injuries to Plaintiff and Class Members resulting from the Data Breach were directly caused by Defendants violation of the statutes described herein.

91. Plaintiff and Class Members are within the class of persons the FTC Act and HIPAA were intended to protect.

92. The type of harm that resulted from the Data Breach was the type of harm the FTC Act and HIPAA were intended to guard against.

93. Defendants failure to comply with the FTC Act and HIPAA and regulations constitutes negligence *per se*

94. Defendants duty to use reasonable care in protecting Plaintiff's and Class Members' confidential Private Information in their possession arose not only because of the statutes and regulations described above, but also because Defendants are bound by industry standards to reasonably protect such Private Information.

95. Defendants breached their duties, and was grossly negligent, by acts of omission or commission, by failing to use reasonable measures and indeed even minimally reasonable measures, to protect the Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of their networks and systems;

d. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiff's and Class Members' Private Information;

f. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

96. But for Defendants acts and omissions described above, constituting a wrongful and negligent breach of Defendants duties owed to Plaintiff and Class Members, the Data Breach and Plaintiff's and Class Members' resulting injuries would have been avoided or at least, mitigated, including because Defendants would have identified the malicious activity and stopped the attack before the malicious actors had a chance to inventory Defendants servers and exfiltrate files containing Plaintiff's and Class Members' Private Information.

97. It was foreseeable that Defendants failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would cause Plaintiff's and Class Members' injuries. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the industry.

98. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in one or more types of injuries to them.

99. As a direct and proximate result of Defendants negligence, Plaintiff and Class Members have suffered and will suffer a host of injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but

not limited to uncompensated necessary lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendants possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

100. As a direct and proximate result of Defendants negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

101. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

102. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all Class Members.

COUNT II: BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

103. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 17, and 21 through 61, as if fully set forth herein.

104. Defendants required Plaintiff and Class Members to provide and entrust their Private Information as a condition of obtaining services from Defendants.

105. When Plaintiff and Class Members provided their Private Information to Defendants, they entered into implied contracts with Defendants pursuant to which Defendants

agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiff and Class Members if and when their Private Information was breached and compromised.

106. Specifically, Plaintiff and Class Members entered into valid and enforceable implied contracts with Defendants when they agreed to provide their Private Information to Defendants.

107. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendants included Defendants promise to protect Private Information they collected from Plaintiff and Class Members, or created on their own, from unauthorized disclosures. Plaintiff and Class Members provided this Private Information in reliance on Defendants promise.

108. Under the implied contracts, Defendants promised and was obligated to (a) provide services to Plaintiff and Class Members; and (b) protect Plaintiff's and Class Members' Private Information that was provided to obtain such services and/or created in connection therewith.

109. Defendants contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information are also acknowledged, memorialized, and embodied in multiple documents.

110. Defendants solicited and invited Plaintiff and Class Members to provide their Private Information as part of Defendants regular business practices. Plaintiff and Class Members accepted Defendants offer and provided their Private Information to Defendant.

111. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants data security practices complied with industry standards and relevant laws and regulations, including the FTC Act and HIPAA.

112. Plaintiff and Class Members who partnered or contracted with Defendants for services and who provided their Private Information to Defendants, reasonably believed and expected that Defendants would adequately employ adequate data security to protect that Private Information. Defendants failed to do so.

113. A meeting of the minds occurred when Plaintiff and the Class Members agreed to, and did, provide their Private Information to Defendants and agreed Defendants would receive payment for, amongst other things, the protection of their Private Information.

114. Plaintiff and Class Members performed their obligations under the contracts when they agreed to pay and provided their Private Information to Defendants.

115. Defendants materially breached their contractual obligations to protect the Private Information it required Plaintiff and Class Members to provide when it failed to implement even minimally reasonable logging and monitoring systems, data encryption protocols, or employee training, among other safeguards, and thus allowed Plaintiff's and Class Members' data to be disclosed to criminal actors bent on identity theft, fraud, and extortion.

116. Defendants materially breached their contractual obligations to deal fairly and in good faith with Plaintiff and Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify them of the Data Breach.

117. Defendants materially breached the terms of their implied contracts, including, but not limited to, by failing to comply with industry standards or the standards of conduct embodied in statutes like Section 5 of the FTC Act and HIPAA, or by failing to otherwise protect Plaintiff's and Class Members' Private Information, as set forth *supra*.

118. The Data Breach was a reasonably foreseeable consequence of Defendants conduct, by acts of omission or commission, in breach of these implied contracts with Plaintiff and Class Members.

119. As a result of Defendants failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains with Defendants, and instead received services of a diminished value compared to that described in the implied contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

120. Had Defendants that their data security was inadequate or that they did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have contracted with Defendants.

121. Plaintiff and Class Members would not have provided their Private Information to Defendants in the absence of the implied contracts between themselves and Defendants.

122. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

123. Defendants breached the implied contracts they made with Plaintiff and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely or adequate notice that their Private Information was compromised in and because of the Data Breach.

124. As a direct and proximate result of Defendants breaches of their implied contracts with Plaintiff and Class Members and the attendant Data Breach, Plaintiff and Class Members have

suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendants.

125. Plaintiff and Class Members, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

126. Plaintiff and the Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate credit monitoring to all Class Members.

COUNT III: BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

127. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 17, and 21 through 61, as if fully set forth herein.

128. Given the relationship between Defendants, on one hand, and Plaintiff and Class Members, on the other hand, wherein Defendants served as a guardian of Plaintiff's and Class Members' Private Information, Defendants were in a position of trust and confidence vis-à-vis Plaintiff's and Class Members and became their fiduciary in their undertaking to collect and maintain their Private Information.

129. As Plaintiff's and Class Members' fiduciary, Defendants were obligated to act primarily for Plaintiff and Class Members to (a) safeguard their Private Information in their custody; (b) timely and adequately notify Plaintiff and Class Members of a Data Breach and disclosure of their Private Information; and (c) maintain complete and accurate records of what information (and where) Defendants did and does store.

130. Defendants had and have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendants' relationship with them—especially to secure their Private Information.

131. Due to the imbalance of power and superiority between themselves and Defendants, Plaintiff and Class Members placed their trust and confidence in Defendants, sophisticated business entities, to adequately safeguard the Private Information it collected and maintained from consumers.

132. Defendants accepted the trust and confidence placed in it by Plaintiff and Class Members and received their Private Information based on the mutual understanding that Defendants owed corresponding fiduciary duties to protect it from unauthorized disclosure.

133. Because of the highly sensitive nature of the Private Information they provided to Defendants, Plaintiff and Class Members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendants position, to retain their Private Information had they known the reality of Defendants inadequate data security practices.

134. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect their Private Information from unauthorized disclosure.

135. Defendants also breached their fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach at all, let alone in a reasonable and practicable period.

136. As a direct and proximate result of Defendants failure to prevent, detect, or avoid the Data Breach from occurring by, *inter alia*, following industry standard information security practices to secure Plaintiff's and Class Members' Private Information, Plaintiff's and Class

Members' Private Information was disclosed and misappropriated to unauthorized third parties in the Data Breach without Plaintiff's and Class Members' authorization.

137. The injuries and harm Plaintiff and Class Members suffered were the reasonably foreseeable result of Defendants breach of their fiduciary duty to adequately secure Plaintiff's and Class Members' Private Information.

138. But for Defendants wrongful disclosure of Plaintiff's and Class Members' Private Information in violation of the trust and confidence Plaintiff and Class Members placed in Defendants and Defendants resulting fiduciary duties owed to Plaintiff and Class Members, their sensitive and confidential Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties in the Data Breach, and their injuries would have been avoided and/or mitigated.

139. As a direct and proximate result of Defendants breaches of Plaintiff's and Class Members' confidence, Plaintiff and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to uncompensated necessary lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendants possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

140. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

141. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) provide adequate credit monitoring to all Class Members.

COUNT IV: UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

142. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 17, and 21 through 61, as if fully set forth herein.

143. This claim is pleaded in the alternative to the claim of breach of implied contract.

144. Plaintiff and Class Members conferred direct benefits upon Defendants in the form of agreeing to provide their Private Information to Defendants, without which Defendants could not perform the services they provide.

145. Defendants appreciated or knew of these benefits it received from Plaintiff and Class Members. Under principles of equity and good conscience, Defendants should not be allowed to retain the full value of these benefits—specifically, the costs it saved by failing to implement reasonable or adequate data security practices with respect to the Private Information it collected from Plaintiff and Class Members.

146. After all, Defendants failed to adequately protect Plaintiff's and Class Members' Private Information. And if such inadequacies were known, then Plaintiff and Class Members would never have agreed to provide their Private Information, or payment, to Defendants.

147. Defendants should be compelled to disgorge into a common fund, for the benefit of Plaintiff and the Class, all funds that were unlawfully or inequitably gained despite Defendants misconduct and the resulting Data Breach.

COUNT V: INVASION OF PRIVACY

(On Behalf of Plaintiff and the Class)

148. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 17, and 21 through 61, as if fully set forth herein.

149. Plaintiff and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to Defendants protection of the Private Information in their possession from disclosure to unauthorized actors.

150. Defendant owed a duty to consumers, including Plaintiff and Class Members, to keep their Private Information confidential and secure.

151. Defendants failed to protect Plaintiff's and Class Members' Private Information and instead exposed it to unauthorized persons which is now publicly available, including through the publication of such information to the Dark Web where cybercriminals go to find their next identity theft and extortion victims.

152. Defendants allowed unauthorized third parties access to and examination of the Private Information of Plaintiff and Class Members, by way of Defendants failure to protect the Private Information.

153. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and Class Members is highly offensive to a reasonable person and represents an intrusion upon Plaintiff's and Class Members' seclusion as well as a public disclosure of private facts.

154. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Private Information to Defendants as a condition of receiving services, but did so privately, with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and

Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

155. Through the intrusion, Defendants permitted Plaintiff's and Class Members' Private Information to be published online to countless cybercriminals whose mission is to misuse such information, including through identity theft and extortion.

156. Defendants were fully aware that a failure to implement industry standard cybersecurity safeguards was substantially certain to lead to the disclosure of Plaintiff's and Class Members' sensitive Private Information.

157. The Data Breach constitutes an intentional or reckless interference by Defendants with Plaintiff's and Class Members' interests in solitude or seclusion, as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

158. Thus, Defendants acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were inadequate and insufficient.

159. Defendants acted with reckless disregard for Plaintiff's and Class Members' privacy when it allowed improper access to its systems containing Plaintiff's and Class Members' Private Information without protecting said data from the unauthorized disclosure, or even encrypting such information.

160. Defendants knew of the risk of a data breach but failed to adequately safeguard its systems to prevent the unauthorized release of Plaintiff's and Class Members' Private Information.

161. Because Defendants acted with this knowing state of mind, it had notice and knew of the inadequate and insufficient information security practices would injure and harm Plaintiff and Class Members.

162. As a direct and proximate result of Defendants acts and omissions set forth above, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer injuries and damages as set forth herein, including, without limitation, (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to uncompensated necessary lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which (i) remains unencrypted and available for unauthorized third parties to access and abuse; and (ii) remains in Defendants possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

163. Unless and until enjoined, and restrained by order of this Court, Defendants wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Private Information maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for judgment as follows:

A. An Order certifying this case as a class action, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief in the form of additional technical and administrative cybersecurity controls as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding attorneys' fees and costs, as allowed by law,

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

I. Any and all such relief to which Plaintiff and the Class are entitled.

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: May 15, 2025

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
214-744-3000
214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

Casondra Turner *
MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (866) 252-0878
Fax: (771) 772-3086
cturner@milberg.com

* *Pro hac vice forthcoming*

Counsel for Plaintiff and the Proposed Class